UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/281,042	03/30/1999	SEIKI AGURO	TIJ-26495	6678

23494 7590 04/07/2004

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
JONES, HUGH M	

ART UNIT	PAPER NUMBER
2128	32

DATE MAILED: 04/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 32

Application Number: 09/281,042
Filing Date: March 30, 1999
Appellant(s): AGURO, SEIKI

William B. Kempler
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 1/20/2004.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. There are no related appeals or interferences.

(3) Status of Claims

The statement of the status of the claims contained in the brief is incorrect. Appellants' commentary and recitation of the prosecution history is irrelevant to the *status of the claims*, is inaccurate, and appears to be nothing more than an attempt to *complain* about non-appealable issues.

A correct statement of the status of the claims is as follows:

Claims 4-21 stand rejected.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is incorrect for the following reasons:

- The objections to the claims is withdrawn.
- Appellants refer to an amendment mailed 2/19/2002. The Examiner, respectfully, is not aware of such an amendment. The paper most closely associated with such a date is an Appeal Brief (paper # 19 – 3/5/2002).
- Appellants also amended the claims in paper # 27 (8/12/2003).

(5) Summary of Invention

The summary of invention contained in the brief is not agreed with.

Appellants begin the exposition by inferring that the claimed invention pertains to a "one-chip" computer environment (first paragraph, page 3, paper # 31 – Appeal Brief). A single chip computer system simply *has not been claimed.* The claims recite (preambles) "integrated circuit computer system". They do not recite a "single chip integrated computer system" or a "integrated computer system on a single chip". If the argument is that the solution in the "fixed system environment" fails in the "one-chip computer environment", then the limitations must be claimed in the proper context, namely, a single chip integrated computer system.

Furthermore, Appellants allegations regarding advantages of the invention (see second full paragraph (page 3, paper # 31 – Appeal Brief) appear to be an attempt to inappropriately introduce argument.

(6) Issues

The appellant's statement of the issues in the brief is susbstantially correct. The 112(2) rejections have been withdrawn.

(7) Grouping of Claims

Appellant's brief includes a statement that the claims do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

4,700,296	Palmer et al.	10/1987
5,960,084	Angelo	9/1999

5,774,545	Raghavachari	6/1998
5,784,577	Jacobson et al.	7/1998
5,357,572	Bianco et al.	10/1994

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 8, 10, 14-15 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Palmer, Jr. et al. U.S. Patent 4,700,296.

As regards Claim 8 the Palmer, Jr. et al. reference discloses an integrated circuit computer system (Figure 2, Item 6i) having a processor interconnected with memory (Figure 1, Item 6d and Col. 5 Lines 32-65) and peripheral circuits on said integrated circuit (Figure 1 Items 6f and 6c and 6a) coupled to a security system (Figures 1-6 and Col. 1 Lines 30-61) comprising:

a plurality of input ports for said processor, (Figure 1 Items 6b, 6c, 6d, 6e note the direction of the arrows to the Process Control Program and Col. 2 Lines 50-68 and Col. 3 Lines 1-4).

a program stored in said memory to operate said processor (Figure 1, Process Control Program and Item 6d Code Table (ROM)), to receive a plurality of commands to said plurality of input ports to produce a password (Figure 1 Items 6c, Item 4 and Figure 2 Item 6c and Figure 4 and Figure 5 and Col. 1 Lines 37-56 and Col. 5 Lines 32-65) which is compared with a predetermined password (Figure 2 Item labeled LOOK-UP TABLE and Col. 7 Lines 33-38).

As regards Claim 10, the Palmer, Jr. et al. reference inherently discloses a specified time sequence.

As regards Claim 14, Palmer Jr. et al. reference teaches; A security system for an integrated circuit computer system (All of Figures 1, 2 and 3 and Col. 2 Lines 50-54) comprising: applying a plurality of commands to a plurality of ports for a processor of said system (Figure 1 Items 6a, the block labeled PROCESS CONTROL PROGRAM, Item 4, Item 6f); a program stored in a memory coupled to said processor for operating said processor to process said plurality of commands to produce a password; (Figure 2 Item 6i and Item 6c and Col. 1 Lines 37-56); comparing said produced password with a predetermined password (Figure 1 Item 6 PARAMETER STORAGE REGISTERS, and Figure 2, Item 6i PARAMETER STORAGE and Col. 8 Lines 12-32).

Claims 8, 10, 14-15 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Angelo.

Angelo discloses a method for enabling power to all or portions of a computer system based upon the results of a two-piece user verification process that is completed as part of a secure power-up procedure. ***At some point during the secure power-up procedure, the computer user provides an external token or smart card that is coupled to the computer through specialized hardware.*** The token or smart card is used to store an encryption algorithm furnished with an encryption key that is unique or of limited production. ***The computer user is then required to enter a plain text user password. Once entered, the user password is encrypted using the encryption algorithm contained in the external token to create a system password. The***

system password is compared to a value stored in secure memory. If the two values match, the power-on sequence is completed and power to the computer system and/or secured computer resources is enabled. If the two values do not match, power to the entire computer system and/or secured computer resources is disabled. The two-piece nature of the authorization process requires the presence of both the user password and the external token in order to generate the system password. ***Angelo also discloses (col. 9) that when the user is prompted to enter a plain text power-on password, as an alternative to a memorized value, the plain text password could be generated with the aid of biometrics. For example, a scanned fingerprint could be converted into a plain text password value***. See col. 1-2 for general background; col. 3, lines 16-36; fig. 2 and corresponding text; col. 7-9.

Claims 4, 5, 9 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Palmer, Jr. et al. U.S. Patent 4,700,296 in view of Raghavavhari U.S. Patent 5,774,545.

As regards Claim 4 the Palmer, Jr. et al. reference discloses an integrated circuit computer system (Figure 2, Item 6i) having a processor interconnected with memory (Figure 1, Item 6d and Col. 5 Lines 32-65) and peripheral circuits on said integrated circuit (Figure 1 Items 6f and 6c and 6a). A security means (Figures 1-6 and Col. 1 Lines 30-61) comprising: a plurality of input ports for said processor (Figure 1 Items 6b, 6c, 6d, 6e note the direction of the arrows to the Process Control Program and Col. 2 Lines 50-68 and Col. 3 Lines 1-4); a program stored in said memory to operate said processor (Figure 1, Process Control Program and Item 6d Code Table (ROM)), to

receive a plurality of commands to said plurality of input ports to process said commands to produce a password (Figure 1 Items 6c, Item 4 and Figure 2 Item 6c and Figure 4 and Figure 5 and Col. 1 Lines 37-56 and Col. 5 Lines 32-65) which is compared with a predetermined password (Figure 2 Item labeled LOOK-UP TABLE and Col. 7 Lines 33-38), and a switching circuit is responsive to said comparison (Col. 4 Lines 36-50).

The Palmer, Jr. et al. reference does not expressly disclose, a scan-path interface circuit for reading out the predetermined memory or register in said system.

The Raghavachari reference discloses that many integrated circuits are accessed via scan ports and specifically discloses a scan-path interface circuit (Figure 1 Item 15 and Col. 13 Lines 10-13) as part of a security system requiring password authentication through comparison of an input password from an external device with a pre-stored password (Figures 1-10 and Col. 13 Lines 4-67 and Col. 14 Lines 1-67 and Col. 15 Lines 1-29 and Col. 16 Lines 1-29).

It would have been obvious to one of ordinary skill in the art, at the time of the invention, to have combined the Palmer, Jr. et al. reference with the Raghavachari reference because, (motivation to combine) by protecting the scan-path interface with a password the integrated circuit is rendered useless to those who cannot meet the random security challenge and therefore reduces the value of the integrated circuit to potential thieves, (Raghavachari, Col. 1 Lines 45-61).

As regards Claim 9 the Palmer, Jr. et al. reference does not expressly disclose a switching circuit coupled to said scan-path interface.

The Raghavachari reference discloses that many integrated circuits are accessed via scan ports and specifically discloses a switching circuit coupled to said scan-path interface (Figure 1 Items 15 and 13, Figure 5 Items 56, 55, 51, Figure 8 Items 81, 82, 83 and Col. 2 Lines 60-67, Col. 3 Lines 1-40), and responsive to said comparison for switching said scan-path interface circuit (Figure 5 and Col. 7 Lines 30-41), between a first mode in which it is enabled (Figure 9, note the control flow diamond decision symbol that states "PASSWORDS MATCH?" after this symbol, follow the arrow for the, YES result, to the computational steps rectangle symbol wherein, the item labeled "1. UNLOCK THE DEVICE") and a second mode in which it is disabled (Figure 9, note the control flow diamond decision symbol that states "PASSWORDS MATCH?" after this symbol, follow the arrow to the, NO result to the computational steps rectangle symbol wherein, the item labeled "1.INCREMENT FAILURE COUNT REGISTER, follow the arrows in the flow chart to the control decision symbol that states "SECURITY PASSWORD RECEIVED" and note that a, NO result, creates a loop back into that control decision symbol and NEVER sets the needed bits in the SECURITY STATUS REGISTER required to enable the scan-path port to operate).

It would have been obvious to one of ordinary skill in the art, at the time of the invention, to have combined the Palmer, Jr. et al. reference with the Raghavachari reference because, (motivation to combine) by protecting the scan-path interface with a password the integrated circuit is rendered useless to those who cannot meet the random security challenge and therefore reduces the value of the integrated circuit to potential thieves, (Raghavachari, Col. 1 Lines 45-61).

As regards Claims 5, the Palmer, Jr. et al. reference inherently discloses a specified time sequence.

The Raghavachari reference also discloses receiving a plurality of commands which are applied to said plurality of ports in a specific time sequence (Figures 9, 10 and Col. 9 Lines 49-66, Col. 10 Lines 1-67, Col. 11 Lines 1-67, Col. 12 Lines 1-60).

Claims 6, 7, 11, 12, 13, 16, 17, 19, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Palmer, Jr. et al. U.S. Patent 4,700,296 in view of Raghavavhari U.S. Patent 5,774,545 and in further view of Jacobson et al. U.S. Patent 5,784,577.

As regards Claims 6, 7, 11, 12, 13, 16 and 17 the Palmer et al. reference does not expressly disclose; a pair of registers, one of said registers receiving said produced password and the other of said registers containing said predetermined password; and a comparator for comparing the contents of said registers.

The Jacobson et al. reference discloses; a pair of registers (Figure 3, Items 301 and 302), one of said registers receiving said produced password (Figure 3 Item 302) and the other of said registers containing said predetermined password (Figure 3 Item 301) a comparator for comparing the contents of said registers (Figure 3 Item 303) for controlling a Data Protect Circuitry (Figure 3 Item 306).

It would have been obvious to one of ordinary skill in the art, at the time of the invention, to have combined the Palmer, Jr. et al. reference with the Jacobson et al. reference because, (motivation to combine) a need arises for an accurate, overridable

method of tracking versions of the PLDs, as well as preventing unauthorized users from programming the PLDs, (Jacobson et al. Col. 2 Lines 10-13).

As regards Claims 19, 20 and 21, the Palmer, Jr. et al. reference does not expressly disclose; a scan-path interface circuit for comparison with a predetermined memory or register, and a switching circuit that is responsive to said comparison to switch operation of said scan-path interface between enabled and disabled modes. (It is noted by the examiner that the Palmer, Jr. et al. reference does disclose a switching circuit and a comparison of a predetermined memory or register, responsive to said comparison of an externally provided password with a predetermined password, the ONLY limitation not disclosed in the Palmer, Jr. et al. reference is a scan-path interface).

The Jacobson et al. reference discloses a scan-path interface circuit (Col. 1 Lines 42-55, Col. 4 Lines 39-42) for reading out contents of a predetermined memory or register in said system (Figure 3, Item 300 and Col. 2 Lines 15-45) and a switching circuit responsive to said comparison to switch operation of said scan-path interface between enabled and disabled modes, (all of Figure 3 and Figure 2 and Col. 3 Lines 14-67, Col. 4 Lines 1-49).

It would have been obvious to one of ordinary skill in the art, at the time of the invention, to have modified the Palmer, Jr. et al. reference with the Jacobson et al. reference because, (motivation to combine) ...a need arises for an accurate, overridable method of tracking versions of the PLDs, as well as preventing unauthorized users from programming the PLDs (Jacobson et al. Col. 2 Lines 11-13).

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Palmer, Jr. et al. U.S. Patent 4,700,296 view of Jacobson et al. U.S. Patent 5,784,577.

The Palmer, Jr. et al. reference does not expressly disclose; a scan-path interface circuit for comparison with a predetermined memory or register, and a switching circuit that is responsive to said comparison to switch operation of said scan-path interface between enabled and disabled modes. (It is noted by the examiner that the Palmer, Jr. et al. reference does disclose a switching circuit and a comparison of a predetermined memory or register, responsive to said comparison of an externally provided password with a predetermined password, the ONLY limitation not disclosed in the Palmer, Jr. et al. reference is a scan-path interface).

The Jacobson et al. reference discloses a scan-path interface circuit (Col. 1 Lines 42-55, Col. 4 Lines 39-42) for reading out contents of a predetermined memory or register in said system (Figure 3, Item 300 and Col. 2 Lines 15-45) and a switching circuit responsive to said comparison to switch operation of said scan-path interface between enabled and disabled modes, (all of Figure 3 and Figure 2 and Col. 3 Lines 14-67, Col. 4 Lines 1-49).

It would have been obvious to one of ordinary skill in the art, at the time of the invention, to have modified the Palmer, Jr. et al. reference with the Jacobson et al. reference because, (motivation to combine) ...a need arises for an accurate, overridable method of tracking versions of the PLDs, as well as preventing unauthorized users from programming the PLDs (Jacobson et al. Col. 2 Lines 11-13).

Claims 4-7, 9, 11-13, 16-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo in view of Bianco et al..

Angelo discloses a method for enabling power to all or portions of a computer system based upon the results of a two-piece user verification process that is completed as part of a secure power-up procedure. ***At some point during the secure power-up procedure, the computer user provides an external token or smart card that is coupled to the computer through specialized hardware.*** The token or smart card is used to store an encryption algorithm furnished with an encryption key that is unique or of limited production. ***The computer user is then required to enter a plain text user password. Once entered, the user password is encrypted using the encryption algorithm contained in the external token to create a system password. The system password is compared to a value stored in secure memory***. If the two values match, the power-on sequence is completed and power to the computer system and/or secured computer resources is enabled. If the two values do not match, power to the entire computer system and/or secured computer resources is disabled. The two-piece nature of the authorization process requires the presence of both the user password and the external token in order to generate the system password. *Angelo also discloses (col. 9) that when the user is prompted to enter a plain text power-on password, as an alternative to a memorized value, the plain text password could be generated with the aid of biometrics. For example, a scanned fingerprint could be converted into a plain text password value.* See col. 1-2 for general background; col. 3, lines 16-36; fig. 2 and corresponding text; col. 7-9.

Angelo does not expressly disclose; a *scan-path* interface circuit for comparison with a predetermined memory or register, and a switching circuit that is responsive to said comparison to *switch operation of said scan-path* interface between enabled and disabled modes.

Bianco et al. disclose a set/scan test capability which is provided for a circuit that includes sensitive subcircuits, but that can be latched out to prevent reverse engineering the sensitive elements. A mechanism to inhibit set/scan test access to at least some of the sensitive subcircuits is selectively actuated by a control circuit to override a normal set/scan test and inhibit set/scan access to the sensitive subcircuits. Various implementations are possible, such as fusible-link PROMs for irreversibly inhibiting set/scan access to the sensitive subcircuits after an initial non-inhibited test period, the use of encryption codes to enable repeated set/scan access to the sensitive subcircuits, and an erasable/reprogrammable mechanism for inhibiting set/scan access to programmed sets of subcircuits. See col. 1 to col. 2, line 26 for need to protect integrated circuits; col. 2, line 29 to col. 3, line 8; fig. 6 and corresponding text.1

It would have been obvious to one of ordinary skill in the art, at the time of the invention, to have modified the Angelo reference with the Bianco et al. reference (motivation to combine) for the following reasons. Bianco states that integrated circuitry is subject to reverse engineering and should be protected (col. 1-2). Bianco discloses enhancing the testability of ICs that contain sensitive circuitry through the use of the set/scan test technique, while preventing the disclosure of the sensitive circuitry design to unauthorized parties. In so doing the invention allows sensitive subcircuits to be

removed from the set/scan test chain. The removal can be permanent, or the sensitive subcircuits can be included in the set/scan chain in response to the application of a control code by an authorized user. The manufacturer is provided with full testability during device fabrication, while access to the sensitive elements can be restricted once the device is delivered; copiers are thereby prevented from exploiting the set/scan capability to obtain design details required for the production of unauthorized copies. The invention is compatible with, and enhances the strength of, other anti-reverse engineering measures such as opaque die coatings or the techniques disclosed in U.S. Pat. No. 4,766,516. Bianco discloses the need for a mechanism to inhibit set/scan test access to at least some of the IC's sensitive subcircuits, and a mechanism for overriding a normal set/scan test by actuating the inhibit mechanism for the sensitive subcircuits while permitting set/scan access to the remaining subcircuits.

(11-a) Response to Argument - 112 (2) rejections

Appellant's arguments pertaining to the missing steps/structural elements are, respectfully, not understood. Appellants' arguments do not appear to address the merits of the rejections. However, the issue is moot because the rejections have been withdrawn.

(11-b) Response to Argument – prior art rejections

Appellant's arguments with respect to the claims have been considered but are not persuasive.

Appellant's arguments relating to the Palmer 102 rejection are noted, but are not persuasive. Palmer, Jr. et al. reference discloses an integrated circuit computer system (Figure 2, Item 6i) having a processor interconnected with memory (Figure 1, Item 6d and Col. 5 Lines 32-65) and peripheral circuits on said integrated circuit (Figure 1 Items 6f and 6c and 6a). A security means (Figures 1-6 and Col. 1 Lines 30-61) comprising: a plurality of input ports for said processor (Figure 1 Items 6b, 6c, 6d, 6e note the direction of the arrows to the Process Control Program and Col. 2 Lines 50-68 and Col. 3 Lines 1-4); a program stored in said memory to operate said processor (Figure 1, Process Control Program and Item 6d Code Table (ROM)), to receive a plurality of commands to said plurality of input ports to process said commands to produce a password (Figure 1 Items 6c, Item 4 and Figure 2 Item 6c and Figure 4 and Figure 5 and Col. 1 Lines 37-56 and Col. 5 Lines 32-65) which is compared with a predetermined password (Figure 2 Item labeled LOOK-UP TABLE and Col. 7 Lines 33-38), and a switching circuit is responsive to said comparison (Col. 4 Lines 36-50). Appellants, respectfully, appear to be reading in definitions which are not reflected in the claims. For example, if Appellants feel that port only means " a group of I/O pins...", then that feature should be recited in the claims.

Appellants are also reminded that the claimed invention does not recite a "one-chip" computer environment (first paragraph, page 3, paper # 31 – Appeal Brief). A single chip computer system simply *has not been claimed.* The claims recite (preambles) "integrated circuit computer system". They do not recite a "single chip integrated computer system" or a "integrated computer system on a single chip". If the

argument is that the solution in the "fixed system environment" fails in the "one-chip computer environment", then the limitations must be claimed in the proper context. namely, a single chip integrated computer system.

Appellants conclude their arguments with abstract hypothetical arguments (see page 8, paper # 31 – Appeal Brief, for example) relating to "reversed situations". The Examiner, respectfully, will not address such hypothetical arguments.

Appellant's arguments relating to the Angelo et al. rejection are noted, but are not persuasive. The argument that Angelo does not disclose an integrated circuit computer system is simply not persuasive. Angelo discloses a method for enabling power to all or portions of a computer system based upon the results of a two-piece user verification process that is completed as part of a secure power-up procedure. ***At some point during the secure power-up procedure, the computer user provides an external token or smart card that is coupled to the computer through specialized hardware.*** The token or smart card is used to store an encryption algorithm furnished with an encryption key that is unique or of limited production. ***The computer user is then required to enter a plain text user password. Once entered, the user password is encrypted using the encryption algorithm contained in the external token to create a system password. The system password is compared to a value stored in secure memory***. If the two values match, the power-on sequence is completed and power to the computer system and/or secured computer resources is enabled. If the two values do not match, power to the entire computer system and/or secured computer resources is disabled. The two-piece nature of the authorization

process requires the presence of both the user password and the external token in order to generate the system password. *Angelo also discloses (col. 9) that when the user is prompted to enter a plain text power-on password, as an alternative to a memorized value, the plain text password could be generated with the aid of biometrics. For example, a scanned fingerprint could be converted into a plain text password value.* See col. 1-2 for general background; col. 3, lines 16-36; fig. 2 and corresponding text; col. 7-9.

Furthermore, Appellants are again reminded that the claimed invention does not recite a "one-chip" computer environment (first paragraph, page 3, paper # 31 – Appeal Brief). A single chip computer system simply *has not been claimed.* The claims recite (preambles) "integrated circuit computer system". They do not recite a "single chip integrated computer system" or a "integrated computer system on a single chip". If the argument is that the solution in the "fixed system environment" fails in the "one-chip computer environment", then the limitations must be claimed in the proper context.

The arguments against the 103 rejections are not persuasive. The arguments against Palmer have been addressed earlier.

The Raghavachari reference discloses that many integrated circuits are accessed via scan ports and specifically discloses a scan-path interface circuit (Figure 1 Item 15 and Col. 13 Lines 10-13) as part of a security system requiring password authentication through comparison of an input password from an external device with a pre-stored password (Figures 1-10 and Col. 13 Lines 4-67 and Col. 14 Lines 1-67 and Col. 15 Lines 1-29 and Col. 16 Lines 1-29).

It would have been obvious to one of ordinary skill in the art, at the time of the invention, to have combined the Palmer, Jr. et al. reference with the Raghavachari reference because, (motivation to combine) by protecting the scan-path interface with a password the integrated circuit is rendered useless to those who cannot meet the random security challenge and therefore reduces the value of the integrated circuit to potential thieves, (Raghavachari, Col. 1 Lines 45-61).

The Raghavachari reference discloses that many integrated circuits are accessed via scan ports and specifically discloses a switching circuit coupled to said scan-path interface (Figure 1 Items 15 and 13, Figure 5 Items 56, 55, 51, Figure 8 Items 81, 82, 83 and Col. 2 Lines 60-67, Col. 3 Lines 1-40), and responsive to said comparison for switching said scan-path interface circuit (Figure 5 and Col. 7 Lines 30-41), between a first mode in which it is enabled (Figure 9, note the control flow diamond decision symbol that states "PASSWORDS MATCH?" after this symbol, follow the arrow for the, YES result, to the computational steps rectangle symbol wherein, the item labeled "1. UNLOCK THE DEVICE") and a second mode in which it is disabled (Figure 9, note the control flow diamond decision symbol that states "PASSWORDS MATCH?" after this symbol, follow the arrow to the, NO result to the computational steps rectangle symbol wherein, the item labeled "1.INCREMENT FAILURE COUNT REGISTER, follow the arrows in the flow chart to the control decision symbol that states "SECURITY PASSWORD RECEIVED" and note that a, NO result, creates a loop back into that control decision symbol and NEVER sets the needed bits in the SECURITY STATUS REGISTER required to enable the scan-path port to operate).

Bianco et al. disclose a set/scan test capability which is provided for a circuit that includes sensitive subcircuits, but that can be latched out to prevent reverse engineering the sensitive elements. A mechanism to inhibit set/scan test access to at least some of the sensitive subcircuits is selectively actuated by a control circuit to override a normal set/scan test and inhibit set/scan access to the sensitive subcircuits. Various implementations are possible, such as fusible-link PROMs for irreversibly inhibiting set/scan access to the sensitive subcircuits after an initial non-inhibited test period, the use of encryption codes to enable repeated set/scan access to the sensitive subcircuits, and an erasable/reprogrammable mechanism for inhibiting set/scan access to programmed sets of subcircuits. See col. 1 to col. 2, line 26 for need to protect integrated circuits; col. 2, line 29 to col. 3, line 8; fig. 6 and corresponding text.1

It would have been obvious to one of ordinary skill in the art, at the time of the invention, to have modified the Angelo reference with the Bianco et al. reference (motivation to combine) for the following reasons. Bianco states that integrated circuitry is subject to reverse engineering and should be protected (col. 1-2). Bianco discloses enhancing the testability of ICs that contain sensitive circuitry through the use of the set/scan test technique, while preventing the disclosure of the sensitive circuitry design to unauthorized parties. In so doing the invention allows sensitive subcircuits to be removed from the set/scan test chain. The removal can be permanent, or the sensitive subcircuits can be included in the set/scan chain in response to the application of a control code by an authorized user. The manufacturer is provided with full testability during device fabrication, while access to the sensitive elements can be restricted once

the device is delivered; copiers are thereby prevented from exploiting the set/scan capability to obtain design details required for the production of unauthorized copies. The invention is compatible with, and enhances the strength of, other anti-reverse engineering measures such as opaque die coatings or the techniques disclosed in U.S. Pat. No. 4,766,516. Bianco discloses the need for a mechanism to inhibit set/scan test access to at least some of the IC's sensitive subcircuits, and a mechanism for overriding a normal set/scan test by actuating the inhibit mechanism for the sensitive subcircuits while permitting set/scan access to the remaining subcircuits.

The argument that the system of Bianco requires more circuitry or is less elegant is, respectfully, irrelevant.

The allegations on page 13 of the Appeal Brief, respectfully, do not distinguish the claims over the prior art.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Hugh Jones Ph. D.

Primary Examiner

April 4, 2004

Conferees

Kevin Teska (SPE)

William Thomson (Primary)

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

HUGH JONES Ph.D
PRIMARY PATENT EXAMINER
TECHNOLOGY CENTER 2100